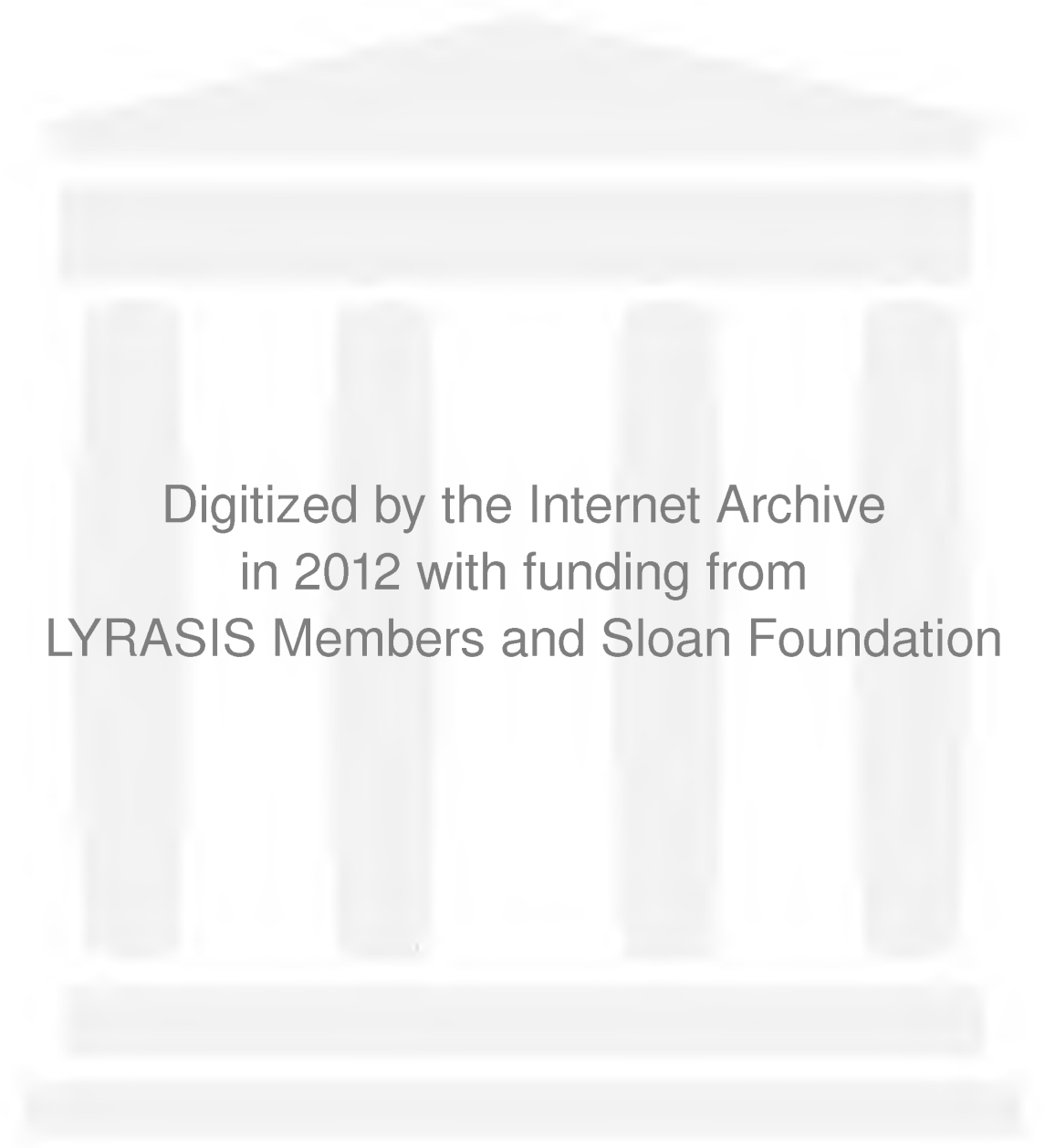
NETWORKS AND NETWORK SECURITY

Michael Kuralt



Networks and Network Security
by
Michael Kuralt

A Thesis Submitted in Partial Fulfillment of
Requirements of the CSU Honors Program

For Honors in the degree of
Computer Information Systems Management
in
Bachelor of Business Administration,
D. Abbott Turner College of Business,
Columbus State University

Thesis Advisor _____ Date 5/01/08

Committee Member _____ Date 05-/01/08

CSU Honors Program Director _____ Date 05/01/08

CIT 6-16-08

TABLE OF CONTENTS

Abstract

In a world of ever-increasing security threats, companies have the difficult task of securing their networks from attack. One of the largest threats to a company is the users on its network. By educating its network administrators and employees about network threats, a company can lower its vulnerability to network attacks. Individual users also can benefit from understanding networks and network security by learning how to keep their computer and their information safe. Companies and users can stay safe by understanding how a network functions, what threats exist on the Internet, how to prevent and deal with attacks, and how to create a secuirty policy to govern proper computer usage.

Purpose of the Thesis

Network security has become a component part of business operations due to the persistent threat of network attacks. Thanks to well written security policies, most businesses are able to function comfortably in the business environment (Singapore, 2002). Although these policies aid in avoiding security compromises, not all businesses are able to maintain the precautionary measures they enact. Apart from the colloquially known network security software (such as firewalls), network security consists of many more components including network reports, hardware and software configuration, systems used by the company, and the very users employed by the company or doing business with the company. Due to all of these factors that can affect network security, it is imperative that even the most technically-challenged people be aware of why certain security policies are enacted (Harrison, 2005). The purpose of this thesis is to increase awareness of network security in the office and at home by educating the public, reinforcing business decisions, and providing guidelines for network security.

Educating the Public

Network security issues can occur for many reasons and user-related mistakes are one of the main causes. It is therefore of the utmost importance that computer users become educated as to how they can help keep a network (and their own computers) safe (Harrison, 2005). Unfortunately, not all users are as computer savvy as others. Therefore, in order to help facilitate the learning process, this thesis will start with network and security basics before moving on to more advanced topics.

Each topic will be introduced at a rudimentary level so that new users can become aware of the new component. Once a new term has been introduced, an example or analogy will be

used to explain the function of the concept. Once introduced, the topic will be explained in depth to create a full understanding of the concept and its functions.

Often users, who are unfamiliar with computer concepts, show a tendency to avoid learning things they consider unnecessary for basic computing needs. Avoiding this information may relieve the frustration of confusion, but remaining ignorant to the computer world while still using computers is a very risky approach, especially in business.

Some major threats circulating around on the Internet include viruses, hackers, and web scams. Although most users – no matter their technical levels – are aware of these threats, most uninformed users simply write off the threats as *bad* while never actually knowing much else about them. Without having at least a basic understanding of how these threats work, a user easily can fall into a trap that could have otherwise been avoided.

Many users will download anything free file they see, which makes them easy targets for viruses (Harrison, 2005). Haphazard downloading is especially problematic with e-mails. What many users do not understand is that threats can exist in more places than just e-mail attachments. The web links present in e-mails can take users to a variety of unsafe places on the web from phishing sites seeking to steal information to sites that sneak a virus onto the computer when a user visits it.

In addition to users unintentionally finding trouble, they can inadvertently give out sensitive information. E-mail again becomes a target for attack. Users who choose to transmit sensitive information over e-mail (e.g. credit card numbers, passwords, or identification numbers) are subjecting their information to possible interception by a malicious third party. The same is true for false websites that were set up to appear like a legitimate site. Information threats will be discussed later in this paper along with ways to identify and avoid them.

Most employees at a company provided with a security policy that governs their computer usage. Often, users resent these policies because they prevent the user from accessing what they want online. The purpose of for security policies is to prevent network security breaches and improper network usage. Thus, it is important for users to understand why these policies are necessary (Noonan, 2004).

Many companies create policies for using passwords. As intended, passwords prevent unauthorized user-access to system resources. Some companies require certain criteria for passwords (upper and lowercase letters or special characters). Password specifications are set in place to make passwords more difficult to guess for intruders. Difficult passwords help prevent people from snooping around where they do not belong (Noonan, 2004).

One of the least favored security policies is internet restriction (Harrison, 2005). The main purpose of blocking websites and services is to protect user and company information and block known malicious websites and programs to prevent security breaches. Some companies choose to block non-malicious websites and services as well simply to keep employees on task. Either way, internet restriction helps maintain computer safety (Andrés & Kenyon, 2004).

Another security policy employed by many companies is to monitor network usage. By overseeing the network, companies are able to detect and stop unwanted users before they can break into the network. While unwanted users are usually outsiders trying to break in to access company information, they sometimes are company employees who attempt to cause trouble from the inside. Monitoring network usage can help prevent both situations (Andrés & Kenyon, 2004).

Reinforcing Business Decisions

Computers are used daily by most businesses in the modern world. Unfortunately, heavy reliance on computers to manage information creates a necessity for network security. Company information is the lifeblood of a company and any loss of that information has the potential of grave consequences for any company. As one would gather, company information also is a key target for many attackers.

Company information is sensitive in terms of how vulnerable it is. The viruses discussed in the previous section have a way of destroying data and making recovery almost impossible. The loss of information can set a company back for several months (or in some cases years) when trying to recover lost data (McAfee & Haynes, 1989).

Unauthorized users can easily change company information if they are able to access it. Company secrets stored on a hacked computer can be discovered and used to the advantage of the hacker. Information also can be altered to a hacker's liking such as removing a balance owed amount.

In addition to company information security, customer information must be kept safe. Some hackers access customer information and sell it to the company's competitors. Additionally, hackers can delete information to hurt company sales. More commonly, hackers attempt to find stored information (e.g. credit card information and other identity information) they can use to commit identity theft. Such security breaches can lead to multi-million dollar lawsuits since the customers confided in the company and were let down by them.

Jeopardized information can take an indirect hit on a company's reputation. In an attempt to keep their information safe, customers tend to avoid companies that are known to have

security issues. A bad reputation is difficult to revoke and often can last a very long time ("Phishing," 2006).

In order to avoid attacks on company information, investing in network security is a necessity. A firewall can be the first line of defense against such attacks as they can prevent unwanted access to company computer systems as well as prevent company employees from performing dangerous actions on the Internet. Also, requiring passwords can help stop intruders from accessing company resources. Requiring frequent password changes can help prevent hackers from easily guessing a user's password (Noonan, 2004).

Employing attack countermeasures is an important step in securing a network. One of the more common defenses is using a reliable virus scanner to prevent malicious programs from destroying data. Virus scanners help keep company computers functioning normally by preventing viruses from altering the operating system files.

Monitoring network traffic is another good way to keep information safe. Knowing what goes in and out of the company network can give administrators a heads-up when something is wrong (Andrés & Kenyon, 2004). Several ways to defer attackers, while still being able to track them will be explained later in the paper.

Companies must have a plan to deal with a network attack. One of the most beneficial fail-safes is to utilize data backups. By backing up data, users can restore files that have been lost for any reason. Although backups are flawed since they are not always up to date, a backup requires a user to only re-enter the new data instead of all of the data that would otherwise be lost without the backup. Another benefit to having a backup system is if a computer fails, there is another working machine that can take its place while the failed one is being repaired. Thus,

backups will help maintain the flow of business if an important server goes down for any reason (Farley, 2005).

Attempting to determine the cause and location of a network attack is important for network security. Using logs created by firewalls, virus scanners, and network monitoring software can help determine when and where an attack took place. Logged information then can be used to close gaps in the security policy and sometimes even apprehend the person responsible for the breach. Logs also make it unnecessary for constant manual network traffic monitoring – a task that is quite unfeasible ("Network Security," 2000).

Finally, once an attack is detected, it is a good idea to alter the company security policy to help prevent the attack from happening again. Changing what programs and information can and cannot be accessed by users as well as changing different software settings in monitoring programs can block previously open and unwanted routes into the network. The key is to prevent undesired access while not preventing necessary business functions (Andrés & Kenyon, 2004).

Provide Guidelines for Network Security Implementation

In order to protect a network full of users, network administrators must create a set of rules to govern network usage. Otherwise, the network users can cause various security problems and even damage company equipment. A security policy is therefore essential for a company to create and enforce to protect itself, its customers, and its employees (Noonan, 2004).

Security policies are delicate in that they have the both ability to protect and to hurt a company. An effective security policy tells users what they can and cannot do on the network in order to keep the company information safe. An ineffective security policy either will not be clear enough to prevent unwanted activity, or will be too strict and will prevent network activity necessary for business ("Network Security," 2000).

Security policies detail the responsibilities of the company IT team, the usage of hardware, the usage of software, and the restrictions on users. The security policy is, in effect, the *constitution* of the company network. By effectively creating a policy, the company can prevent network attacks as well as have an effective plan as to how to deal with successful attacks (Jarmon, 2002).

An important part of creating a security policy is to be able to assess the risks in a network. Security risks can originate from the user, the computer, and the security policy. User risks come from the services that they are allowed to access and the method that they are allowed to transmit information. Computer risks are based on the software that is used on the machine. Policy risks come from too specific or not specific enough rules as well as overlooked security flaws. By properly assessing risks, the security policy can be updated to appropriately fit the company's security needs (Andrés & Kenyon, 2004).

Introduction to Networks

In order to understand network security, users must gain an understanding of the component parts of a network. Networks are composed of nine interconnected elements that all work together to form the transmission system based on a pre-defined network framework (such as the hybrid TCP/IP-OSI architecture). Networks also may be wired or wireless as well as spread across different physical sites. The nine network elements include applications, servers, clients, routers, switches, wireless access points, access lines, trunk lines, and messages (Panko, 2007).

Applications

A network is a transmission system that connects two or more applications running on different computers. Users should keep in mind that the physical computers do not connect to each other, but rather the programs (software) running on the computers create the network connection. Most applications have the ability to connect various systems run by different operating systems such as Windows, Macintosh, Linux, etc. Because they maintain unrestricted data transfer, applications are key to maintaining a network (Panko, 2007).

Servers

Servers are computers that store data that is accessible to a large number of people. Servers can use the same hardware as a normal computer, but due to the large volume of users it must serve, most servers are outfitted with more powerful equipment than a normal-use computer would have. Servers perform various file-sharing functions (e.g. shared documents and programs) as well as store the files that are used when visiting websites.

Many servers are used as dedicated servers. *Dedicated* means that apart from adding or updating the stored files on the server, no people use the server as a normal computer in order to

maximize the system resources for the server functions. Since many servers use specialized equipment to allow a large volume of users to access its files, many companies place the servers in an isolated, temperature-controlled room to prevent people from using the server and to keep its components cool ("Internet System Management," 2000).

Clients

A client is a computer that connects to a server. Most clients are customer computers seeking either goods or information from a company server, but the company employee computers accessing the server are also clients. Client computers require a program capable of connecting with the server which, in most cases, is an internet browser (Panko, 2007).

Routers

Routers are the gateway to and from the Internet. A router's key purpose is to transfer data from one network to another through the Internet. Computers within a network are all connected to the router either directly or through a series of switches. The term *Internet* refers to the sum-total of all networks connected together via routers, while the term *internet* refers to a smaller set of connected networks (Noonan, 2004).

Switches

Switches help bridge the gap between the computers and the router. Since there are limitations to how long cables can be, a computer cannot always be connected to a router by using only one cord. Switches also allow many computers to be connected to a router even though there are limited ports (places to plug the cord into) available on the router. Switches increase the computer limit since only one port needs to be used to connect to the router while the other ports are left available for other computers. Each switch and router has a list of each connected computer so that information can be transferred to the correct destination. Switches

also can connect to other switches to extend the cable distance and add additional space for computers.

Wireless Access Points

Wireless access points are the bridge between a wired network and a wireless network. The access point is connected to a switch or a router and then converts the data into a wireless signal. In order for computers to use a wireless network, they must have a wireless adapter to convert the wireless signal back into the desired data (Panko, 2007).

Access Lines

Access lines are the cords that connect a computer to a switch or a router and will serve only that computer and its data. The cord needs only be long enough to reach the switch or router.

Trunk Lines

Trunk lines are the cords that connect a switch to a router or a switch to a switch. Trunk lines serve many computers' data, often at once. The ability to transfer different data simultaneously is called multiplexing, which is accomplished by combining the data together during transit and sorting it once it reaches its destination. Also, a technique called packet switching helps transfer large amounts of data through the trunk line's limited capacity by breaking up the data during transit and reassembling it at the destination much like a puzzle.

Messages

Messages are the actual data that is sent through a network. A message is referred to as a *packet* since it is sent like a small package through the Internet. Packets contain information similar to an envelope in the mail. The packet will say who the packet is from and to whom the packet should go. In order to reach its destination, the packet usually will travel through several separate networks in order to reach the destination computer ("Network Security," 2000).

During its transit through an individual network, a packet will be given an extra *envelope* with an address to the next network. The extra envelope is referred to as a frame and contains the address of the next router that will bring the packet closer to its destination (Panko, 2007). The framing process is similar to sending a letter in that while the letter is in transit, it will visit several post offices on the way to the recipient. The frame is most simply thought of as the address to the next post office.

The Hybrid TCP/IP-OSI

Given the basic idea of network composition, the next step in understanding networks is to learn about the widely used hybrid Transmission Control Protocol/Internet Protocol-Open Systems Interconnect (TCP/IP-OSI) architecture. The hybrid TCP/IP-OSI architecture is a common framework for network communication that consists of five layers that combines three OSI layers and two TCP/IP layers. The TCP/IP-OSI layers can be compared to as a view of the earth from the ground to space. On the ground, one would see the inhabitants of the planet. As one journeys toward the skies, only larger items such as cars and buildings are visible. When looking at the Earth from the perspective of an airplane's height, one would see only mountains, trees, and open fields. From space, one would see the world as a large sphere with landmasses and water. The same concept applies to hybrid TCP/IP-OSI architecture. Starting from the lowest level is the physical layer (OSI), the data link layer (OSI), the internet layer (TCP/IP), the transport layer (TCP/IP), and the application layer (OSI) (Panko, 2007).

The physical layer. The physical layer, as the lowest layer in networking is concerned only with transmitting data through the actual wires. The act of moving data through wires is called propagation (Panko, 2007). The wires use a binary signal to transmit data which is simply an electrical current that can be read as either a 0 or a 1 by the computer. The signal is subject to

a process called attenuation, which is the gradual weakening of a signal. As the signal propagates, the electrical signal weakens in its voltage. Once the voltage drops below a certain threshold, the binary value of the signal can no longer be interpreted. Therefore, there are limits to how far a signal can propagate before it must be rejuvenated. Signals are rejuvenated by using switches to resend the data once it is read. Signal rejuvenation is similar to a baseball team throwing a ball across the field by using different players to re-throw the ball so that it will reach the other side with less risk of dropping the ball. Another issue affecting signal propagation is called noise. Noise is any outside electrical interference that can alter a signal. Since computers are electronic, there is always potential for noise to occur (Panko, 2007).

Most local networks use a 4-pair UTP cord to transfer data. UTP stands for unshielded twisted pair (Maki, Hamada, Tokuda, Shimoshio, & Kuwabara, 2001). Unshielded refers to the cord not having extra protection against electrical interference, but alternatively costing a great deal less than a shielded cord. The twisted pairs refer to the wires in the cord being twisted together to avoid a problem called crosstalk interference which is caused by signals mixing together from neighboring wires.

The reason that UTP is a popular choice for networks is because they are cheaper than their alternatives. The low UTP price is very important for networks since the cords are limited to 100 meters in length so that attenuation will stay at a manageable level. UTP cables also have different categories that define the transfer speed that the cable is capable of maintaining. The current most popular category is the Cat. 5e cable since it is cheap and fast enough for most networking needs (Panko, 2007).

A faster alternative to UTP cables is fiber optic cables. Fiber optic cables use light in place of electric currents to transmit data. The cables use a core to send the light signals while

using a cladding to keep outside light from entering the core. Fiber optic cables can send data at very high speeds and longer distances than UTP cables. However, fiber optic cables are much more expensive than UTP cables, especially when using the high-grade cables (Panko, 2007).

The data link layer. Also called the Ethernet layer, the data link layer zooms out from the physical layer to include the switches and router. When researching the Ethernet, two terms will arise: IEEE and 802. The Institute for Electrical and Electronics Engineers (IEEE) is a group responsible for creating various standards for electronics. The 802 Committee, as part of the IEEE, is responsible for creating standards for networking. The Ethernet is governed by a subchapter of the 802 Committee deemed the 802.3 Working Group (Gibson, 1990).

One of the major standards in the data link layer is the MAC standard. Each computer has a permanent address for its network card called a Media Access Control (MAC) address. The MAC address also is known as a physical address. The purpose of a MAC address is to send data to and from a specific computer within a single network (Wright, 2003). Building upon the post office metaphor for a frame, the MAC address serves as the address from the post office to the recipient's house. If a message is send to another computer inside the same network, the MAC address also will serve as the address to the destination. Switches, routers, and access points also can use the MAC address to determine where the message originated in order to prioritize simultaneous messages to be sent in an orderly fashion.

Another aspect of the data link layer is the physical placement of the computers and switches which is referred to as topology. In the Ethernet layer, only one route is allowed to exist to a single computer. In other words, the switches between the computer and the router cannot have an alternative set of switches through which the data may travel because a secondary route can cause the data to loop continuously amongst the switches and never reach the computer. The

cause of this potential loop is that the switches do not determine which switch to send the data to next and instead just use the data's address to send the data through the specified port. Therefore, local networks must use a hierarchy topology as there only is one possible route for the data to travel (Panko, 2007).

A hierarchy topology utilizes a parent-child relationship in which each child has only one parent. At the top level of the hierarchy is a single switch. The top switch can have either multiple computers or other switches connected to it. The same rule applies for the subsequent switches. When properly implemented, no computer should have more than one physical route to it in the hierarchy topology. Unfortunately, having only one route to each computer makes the network unreliable. If the top-level switch were to fail, the computers would no longer have a connection to the router and Internet. To combat this problem, a Spanning Tree Protocol (STP) was created to add a backup route for the top-level switch. Although this backup route provides a second route to the computers, the STP will disable the backup route unless the primary switch fails (Andrés & Kenyon, 2004).

The internet layer. Now that the basic layers have been discussed, it is time to introduce the main layers that deal with network security. Zooming out more from the data link layer, there is the internet layer, which is concerned with moving data from one router to the next. Here, transferring data is done by using an IP address.

The Internet Protocol (IP) address is a special address given to a computer temporarily so that it can communicate over the Internet. IP addresses are issued by a Dynamic Host Configuration Protocol (DHCP) server (Noonan, 2004). Each device that connects to the Internet is called a host. Since the IP address is temporary, it will remain dynamic. Therefore, the DHCP server will give each computer the settings necessary to access the Internet. IP addresses are

made up of four sets of numbers ranging from 0-255. Each set of numbers is an address to a different part of a network. In considering a random example of 164.127.38.4, three related addresses can be determined. The 164.127 is the address of the network that the originating computer belongs to such as a college. The 38 refers to the subnet (sub-network) of the originating computer such as a specific classroom. The 4 refers to the actual computer (Panko, 2007). In other words, if several users in the same room were to compare IP addresses in a normally configured network, they would find that the first three sets of numbers in the IP address are the same.

Although most users are not aware of this, IP addresses also are used to visit websites. The site www.google.com must first be translated into an IP address before the website information can be obtained. The address translation is done by a Domain Name System (DNS). Web servers need to retain their IP address so that the address in the DNS will always correspond to the server (Noonan, 2004). In order to keep an IP address, a company must purchase a static IP address which will never change. A domain name also can contain information about a subnet. The mail server for Google can be found at mail.google.com whereas the *mail* prefix specifies a subnet of Google.

The transport layer. Zooming out further from the internet layer, there is the transport layer which is concerned with getting the message from one computer to the other. The transport layer is governed by the Transmission Control Protocol (TCP) (Panko, 2007). TCP is only part of standard network communication that uses a reliable connection. All of the other layers use an unreliable connection which means that each component sends the data as per instruction, but they never actually check to see if the data arrived at its destination. The transport layer is the only reliable layer in the network architecture because reliability costs network resources (Tang,

Andrew, Chiang, & Low, 2008). Imagine an employee during a very busy day at work with colleagues who continue sending enough tasks to keep the employee busy all day. In order to make the sent tasks reliable in a similar way to TCP, the employee would have to take the time to send each colleague a message saying that the task was received. Each confirmation that the employee must send takes away from the time available to work on the tasks. Since networks have limited speed, using a reliable connection will greatly slow the connection. Therefore, TCP only will ensure and later close a connection to be reliable.

One of the most important functions of the transport layer in terms of network security is that it chooses the port from which to send information. Ports, differing from the physical plugs in switches and routers, are application specific identification numbers that describe which application sent a message and which application should receive the message ("Network Security", 2000). Certain *well-known ports* are the common ports used by popular applications. For example, the port used for internet browsers is port 80 (Panko, 2007). In some cases, a router may not know what to do with a certain port. In these cases, the router will simply throw away the message. To remedy this, the router can be instructed to use port forwarding to send messages using that specific port to a certain computer. The reasons ports are important for network security is that open ports are susceptible to attacks from outsiders ("Network Security", 2000). Port security will be discussed in more detail later in the paper.

The application layer. The application layer, as the top layer in the hybrid TCP/IP-OSI architecture, is what most users are acquainted with in some way. Perhaps the most familiar term in the application layer is HyperText Transfer Protocol (HTTP). Beginning any complete web address (http://www.google.com), HTTP defines how an internet browser is to obtain webpage information. Most webpages are made from HyperText Markup Language (HTML), which is

simply the type of code used to create a webpage. HTTP is used by internet browsers such as Internet Explorer and Mozilla Firefox. Internet browsers have the ability to manage website files and display them to the user by using HTTP standards to communicate.

Another familiar type of application is e-mail. Although many regard e-mail as a website-based service, the inner workings of the system are still linked to an application. Originally, e-mails were required to be written in plain text, which meant that there could be no graphics (pictures) and the words could not be boldfaced, italicized, or underlined. After HTML became popular, e-mail capability, expanded to use HTML, enabled e-mails to contain the same materials used on websites. Initially, e-mails were programmed so only English characters could be displayed, a limitation that restricted the use of any special characters. In order to fix this problem, the UNICODE standard is currently being implemented. UNICODE includes many more characters than e-mails could originally support. Unfortunately, this standard is still a work in progress so most users cannot use UNICODE properly (Panko, 2007).

E-mail is sent by using SMTP. Simple Mail Transfer Protocol (SMTP) requires that an e-mail be sent to the sender's mail server, then to the receiver's mail server, and finally to the receiver's computer. In order to receive messages, one of two other standards must be used: Post Office Protocol (POP) or Internet Message Access Protocol (IMAP). Both of these protocols allow users to download their messages from the mail server to their computer ("Security Auditing, Attacks," 2000). In order to do so, client computers will need a mail application such as Microsoft Outlook. Alternatively, e-mail can be done through HTML which is known as web mail. Web mail allows mobile users to access their mail without needing an extra application, but it is often slower than application-based mail since the web mail server is farther away and heavily used by others.

Over the past few years, another networked service has become immensely popular. Almost every business now offers a form of electronic commerce (e-commerce) so that they can buy and sell goods and services online. E-commerce is fueled by the website's online catalog which shows the goods available for sale. The online catalog is usually maintained by an e-commerce application since the catalog requires constant updates. Companies also rely on an application to manage the customer's *shopping cart*, checkout, and payment for the goods. Without proper management of these functions, e-commerce would not be able to exist as a reliable purchasing method. In order to promote e-commerce, many companies use Customer Relationship Management (CRM) to analyze customer buying trends and other preferences in order to increase sales (Panko, 2007).

Another popular type of application is Peer to Peer (P2P) applications. P2P allows for files to be transferred from one computer (peer) to another. Programs such as instant messengers allow P2P transfer. In some cases, a third-party server helps facilitate the transfer by providing a connection between the two computers. The server, however, does not control any aspect of the transfer except for the server's speed limitations. P2P networks have a disadvantage since a connection cannot be created unless both computers are active. Therefore, P2P networks are not viable alternatives to using a file server (Panko, 2007).

Wireless Networks

Before delving into network security, it is important to cover the subject of wireless networks since it is becoming very popular for mobile users. Wireless networks use the same concepts of wired networks, but they use different technology. As one may recall from earlier in the paper, a wireless network is connected to the wired network via a wireless access point. Only at the access point does the network become wireless. The access point converts the electrical

signals into radio signals and vice versa. Also, in order to use the wireless network, the computer must be outfitted with a wireless network card. Wireless cards can translate the radio signals back into electric signals for the computer to use ("Link Layer and Network Layer," 2003).

A wireless network uses antennas to send and receive the radio waves. Wireless network antennas are Omni-directional which means that they can send and receive signals from all directions at an equal strength. Unfortunately, multi-directional transmission comes at the cost of distance. Therefore, a Wireless Local Area Network (WLAN) is limited to a very short distance due to attenuation. In addition to a weakening signal, WLANs are subjected to other propagation difficulties ("Link Layer and Network Layer," 2003). A shadow zone, or dead spot, is an area that is blocked off from the radio signal by a large solid object such as a wall or a bookcase. Radio signals also are susceptible to electronic interference from other devices such as microwaves and telephones. The largest problem that WLANs face is called multipath interference. Since radio waves can bounce off of objects, a computer may receive the same signal at different times which will cause an issue with interpreting the signal. All of these problems are necessary to consider when setting up a WLAN (Panko, 2007).

Radio signals use certain frequencies called bands. The radio in a car also uses the same bands, but at a much lower frequency. Wireless must use a range of unlicensed bands that do not require special usage permission and that are at higher frequencies than those used by other radio systems. The higher the frequencies of wireless signals, the faster the data transfers, but the high frequency radio waves are extremely sensitive to the WLAN problems mentioned previously. Conversely, lower frequencies are very strong against the WLAN problems, yet provide very slow data transfers. Therefore, most WLAN technologies use what is referred to as *the golden zone*, a range of frequencies that can provide the best wireless service (Panko, 2007, p. 244).

Wireless is convenient because it does not require a computer to use a cable to connect to the internet. Unfortunately, the wireless connection makes it more difficult to manage who has access to an internet connection. Whereas a wired LAN requires each computer to have a physical connection to a switch or router, a WLAN requires only that a computer be in range of the signal, even if a user is outside of the building. Inherently, a wireless network has a number of security threats ("Link Layer and Network Layer," 2003).

One of the security threats of WLANs is called a drive-by hacker: individuals who sit outside a building to gain access to a wireless network connection and then attempt to break into the network as a spy or to attack the network. Other hackers, called war drivers, drive around an area looking for an unprotected wireless connection to infiltrate. Some hackers create an 'evil twin access point' that is disguised to look like a company's access point in order to trick employees into connecting to it so that the hacker can steal data. Lastly, some employees may set up a rogue access point to enable a wireless connection. However rogue access points usually are not secure and can provide an easy entrance to the network for hackers (Panko, 2007).

In order to combat these threats, there are a series of security features that WLANs can have implemented. In the early days of wireless networks, the Wired Equivalent Privacy (WEP) standard was created to prevent users without a network 'key' from accessing the connection ("Link Layer and Network Layer," 2003). Unfortunately, WEP was not very secure since everyone had the same, unchanging key. Soon, a new security standard was created. The Wireless Protected Access (WPA) and standard used a much stronger network key to restrict access. 802.11, which is the IEEE wireless workgroup, created another security standard, 802.11i, which is often referred to as WPA2 since it is even stronger than WPA. Network keys are a type of encryption, which will be covered later in this paper (Panko, 2007).

Virtual Private Networks

The Virtual Private Network (VPN), the last type of network that will be discussed, allows a company to access its network from a different (remote) location. As opposed to a Wide Area Network (WAN) which uses long sets of cables to physically connect each location, a VPN uses the Internet to connect each location. Since the Internet connects the computers, employees can access the company network from home or from other locations. VPNs also are cheaper than WANs because they do not require a third-party company to manage the connections. VPNs are sometimes referred to as a company extranet since it expands the company's internal network (intranet) outside the company premises (Noonan, 2004).

Three types of VPNs exist. Remote access VPNs allow an outside user to connect to a company's intranet. Site-to-site VPNs allow a company to connect different branches to the same intranet. Lastly, Host-to-host VPNs allow an outside user to connect to an inside user (Andrés & Kenyon, 2004). All of these connections require security measures to make sure that the connecting user has permission to access the company network and that no user can intercept the VPN communications.

The most secure standard for VPNs is IP security (IPsec). IPsec can use two modes to connect the computers. In transport mode, IPsec requires that each connecting computer have a digital certificate to prove that it has permission to access the network. Digital certificates must be issued by a third-party certificate authority at a costly fee. All of the data sent using IPsec is encrypted which makes the data unreadable by anyone who does not have a key to decrypt the data. In tunnel mode, an extra computer is used as an IPsec gateway that attempts to secure the internet connection (tunnel) while not requiring any of the computers to have a digital certificate. Tunnel mode is, of course, less secure than transport mode ("Network Security," 2000).

Another security standard available for VPNs is Secure Socket Layer/Transport Layer Security (SSL/TLS), the use of which requires that both connecting computers must be capable of SSL/TLS. Fortunately, most every internet browser and web-server application can use SSL/TLS. The SSL/TLS security standard requires users to authenticate themselves to the company network by either providing a username and password, a presenting a digital certificate, or connecting through a SSL/TLS gateway (Panko, 2007).

Networks are complicated both in their components and functionality. Understanding how the nine network elements function together is the basic knowledge necessary to setup a network. All network transmissions are done through a network framework (such as the hybrid TCP/IP-OSI architecture). Although all network connections require security, both wireless and virtual private networks need special security measures to ensure that there is no unauthorized use of their services. Now that a basic overview of network has been covered, the types of network threats can be described in greater detail.

The Necessity of Network Security

Network security is necessary to protect business and individual assets such as servers, databases, e-mail systems, and computer systems. The purpose of network security is to prevent, detect, and remove network threats from a network or computer. Network threats can include direct attacks (such as hacking), social threats (such as phishing), and non-direct attacks (such as viruses).

Most consumers are aware that hardware and software is quite expensive. Why then would individuals/companies want to spend money to purchase equipment such as firewalls and virus scanners that are not required to run a network? The present section will describe why investing in security features is a good idea. Businesses should have a really deep interest in securing their network because their computers store sensitive data that can cost millions to billions of dollars to replace both in hardware cost and loss of business (McAfee & Haynes, 1989).

Business Servers

As discussed earlier, servers are used to serve a multitude of users for a multitude of purposes. It can therefore be readily assumed that keeping a server running is a very, very important necessity. Server information must remain accurate, reliable, and scalable (Farley, 2005).

The accuracy of information must be ensured in order to be useful. Incorrect information is simply not information. Customers and employees who use the information stored on a server are assuming that they are receiving accurate information with which they may make decisions. Inaccurate information will not help them achieve their goals and will therefore drive people

away from the company. Unauthorized data modification must therefore be prevented by all means. A need for unaltered data means that network security must be implemented.

Information also must be reliable, which means that the server must be available to users as much as possible. Computer storage specialists strive for *the five 9's,* which refers to a server being available 99.999% of the time all year. Five 9's means that out of a full year, a server can be down for only five minutes, which includes updating, servicing, and problem solving (Farley, 2005). As one could imagine, five minutes is not nearly long enough to perform these tasks through the duration of a year, but customers and employees expect the server to always be available. In order for a server to be reliable, it must have accurate and accessible data. According to Farley (2005), *A storage system that inadvertently corrupts or loses data is worthless*. In order to ensure that data is not corrupted by a hacker or a virus, companies must, again, invest in network security (p. 6).

Servers also must be scalable. Scalable refers to the ability to increase the capacity and capability of a system without having to purchase a brand new system. Since servers typically contain a large amount of ever-increasing data, they require a very large and upgradable storage capacity. Most casual computer users are used to hearing about gigabytes (GB), but server administrators have to deal with terabytes (1,024 GB) and even petabytes (1,024 TB). Having a computer store these large amounts of data is a huge liability in the case that the computer fails for any reason. The safest way to store data is to have perform backups. However, if something like a virus finds its way into the data backup, all of the data may be lost anyway (Farley, 2005).

Business Databases

Like servers, databases store a large amount of data as well. Data stored in the database is very important for a company because it often contains important information about customers,

employees, and products. If a database file were to become corrupted, all of the data stored within it can no longer be accessed which can come at great costs to the company. Hackers also can steal information from a database to use at his/her own discretion. Securing a database is therefore a very advisable decision ("Security Auditing, Attacks," 2000).

Customer information stored in a database allows businesses to keep track of who their customers are. Some businesses use customers' past purchase information to retain their business with the customers when a subscription runs out or a new product goes on the market. Customer information can be compromised if it is kept unsecure. Even worse, most hackers who target customer information are after sensitive information such as credit card numbers or other identity-related data. Customers who offer their personal information to a business do so in good faith that the business will protect their information. Failing to do so can relate in lawsuits and turn away customers ("Phishing, 2006").

Databases also may store product information for the business. Losing this data would require the business to re-enter the product information so that customers can purchase the products. Companies also could lose any stored purchase statistics and inventory counts if the database is attacked ("Security Auditing, Attacks," 2000).

Business E-mail

E-mail has become a very popular means of communication in businesses recently. When the boss wants to remind an office of thirty people about the meeting at 10:00 a.m., it is far easier to send an e-mail to everyone instead of tracking each person down individually. Employees also use e-mail to store important information and business contacts ("Security Auditing, Attacks," 2000). If the e-mail system were to be hacked, these luxuries could all be taken away until the problem is resolved. Hackers also could hijack the e-mail system and send out false messages in

the company's name. False messages could be used simply to pester other people or to request customer information in order to steal their identities in the name of the company.

Spam, a big problem in e-mail systems, is unsolicited commercial e-mail that often is sent to thousands of people (Panko, 2007). Most spam recipients know to avoid the messages, yet the few users who open the messages make spamming financially worth-while to the spammer. Spam messages carry commercial offers, spyware, viruses, or phishing attempts, all of which are harmful to a computer and its user as be discussed later in this section. Professional spam messages use special methods to verify an e-mail address. The most common address verification method is to provide an unsubscribe link in a spam message that informs the spammer that the address is being used. Sometimes a graphic within the spam message will inform the spammer that the e-mail was opened when the graphic is downloaded from the spammer's server (Boswell, 2003). Therefore, a user who receives spam should never open the message in order to be protected from receiving more spam.

In order to combat spam, many businesses invest in spam blocking services. Spam blockers use a special set of rules to filter known and possible spam messages. Although spam blockers help lower the number of spam messages on an e-mail server, they also can remove some legitimate messages by accident. Therefore, users must audit the spam folder to ensure that real e-mails were not discarded (Boswell, 2003).

Types of Network Attacks

Front door. As with any form of attack, it would be ideal for an army to be able to just march right in through the front door and take control. Normally, the enemy does not have access to the necessary credentials to use the front door; that is, unless someone was to inadvertently give the enemy those credentials (Andrés & Kenyon, 2004). Sadly enough, something as simple

as keeping a password a secret from others is more of a feat than one might expect. Hackers will attempt to trick people into giving up their passwords through a variety of methods. Some hackers will place a phone call while posing to be a system administrator and ask for the user's password in order to verify their identity. Most companies have a policy against giving out passwords to avoid this trick from happening, but many employees pay no heed to the warnings. Some people will decide to give out their password in person as well. Perhaps employee A was late for a meeting and asks employee B to get a file from a passworded computer. Employee B can then use the password freely without employee A's consent. Hackers also like to use e-mail to trick people into giving out their passwords. The two methods to do this are called phishing and sniffing which will both be discussed later in this section.

Once a hacker obtains the password to a computer system, the hacker can then walk right in the front door of the security *fortress* and wreak havoc. The login screen cannot do anything to block the hacker from entering since it believes that the interloper is a legitimate user. The hacker can then have access to everything that that particular legitimate user had access to as well as have a very advantageous front to stage a deeper attack. Therefore, it is important for companies (and home users) to prevent anyone from giving out their passwords ("Network Security," 2000).

Brute-force. Hackers also use other methods to break into a system. One of the less sophisticated ways to break in is to use brute-force to literally guess the password: a method referred to as brute-force because the process entails trying every single character, number, and symbol that the hacker has the patience to try until the system accepts the password (Noonan, 2004). As one can imagine, this method can take tens of hundreds of fruitless hours and may still not provide a valid password. Brute-force often is assisted by software to automate and greatly

speed up the guessing process. In response to the rare case that brute-force works, most companies make the system lock a user's account if too many failed logins occur so that a hacker cannot continue trying to logon (Noonan, 2004).

An alternative to brute-force is to use a dictionary program to guess the password. Dictionary programs have a list of common passwords that people may use. People who use simple words for passwords are very susceptible to a dictionary program, especially since dictionary programs are much faster than brute-force attacks. Most companies require their passwords to use upper and lowercase letter, a number, and a special character in order to thwart the dictionary program method. Difficult-to-remember and difficult-to-guess password requirements also makes brute-force a very difficult method to use ("Network Security," 2000).

Bugs. Obviously, if an employee does not simply provide a hacker with his/her password, guessing the password is not a very attractive way to break into a system. Most hackers prefer to use more intuitive methods such as a flaw in a program. Program flaws are called exploits because a hacker is able to exploit the flaw in order to break into the system ("Network Security," 2000). For instance, if a burglar knew that the hypothetical I-See-You home security system let all people wearing brown into the house due to a flaw in the system, the burglar could use the exploit to enter the house. The same concept works for breaking into computers. Some programs have an opening or weakness that hackers can use to gain access to a system. Software companies usually release patches to fix these holes, but system administrators are still responsible for applying these patches. Forgetting to update the software can let hackers break in from remote computers ("Security Auditing, Attacks," 2000).

A current example that is claimed by many security specialists to be the most dangerous exploit threat today is the buffer overflow ("Security Auditing, Attacks," 2000). As most users

know, computers have memory just like people. Computer hard drives are like long-term memory and computer RAM is like short-term memory. Computer RAM allows programs to run until the program closes. When a program starts running, it tells the computer how much memory it will need for each function. The computer then gives the program the requested memory and uses the rest of the memory for other functions. The amount of requested memory that the computer allocates for the program is called a buffer. A buffer overflow occurs when the program attempts to use more memory than the computer set aside for it. The effect is similar to a person having to remember too many things short-term and therefore confusing one thing for another. For software, this usually happens due to a program being poorly written ("Buffer Overflow," 2005).

Buffer overflows cause the program to crash which leaves the program vulnerable to be exploited. For example, if a program allows up to 100 characters to be entered into a field, entering more than 100 characters would cause the program to use more memory than it has available. The computer has to do something with the extra characters, so it keeps recording the data which overwrites other program data. When the program crashes from the extra data, it needs to perform extra functions called sub-routines to put things back in order. The extra data from the buffer overflow ends up overwriting the instructions for the sub-routine. If the extra data that a hacker enters contains instructions that the computer can follow, when the extra data overwrites the sub-routine instructions, the computer will have to follow the hacker's instructions instead which can initiate various forms of computer attacks or simply tell the computer to delete everything on its hard drives ("Buffer Overflow," 2005).

More practically stated; a hacker using buffer overflow would be similar to a guest at an over-crowded restaurant inviting more people to the establishment. The poorly coded program is

represented by a new employee working alone in the restaurant. As more people enter the restaurant, the single employee becomes unable to serve the customers, which represents the program crashing. The hacker would be the malicious customer who invited extra people while the restaurant was crowded. Since the employee is busy with the guests, the malicious customer can proceed to use the confusion and chaos to replace the restaurant layout chart with an incorrect version. The new employee, not knowing any better, would use the false instructions to clean up and re-order the restaurant incorrectly. The malicious customer could then bring in a health inspector who would then shut down the disorderly restaurant. Although this example is difficult to imagine in real life, it should help clarify exactly what happens with a buffer overflow.

Back door. When the front door is locked and the system programs are strong against exploits, the next choice of action for a hacker to use the back door. Computer systems do not have a back door for hackers to try to log into just like a front door. Instead, hackers have to create these doorways by using special programs that usually come in the form of a virus ("Network Security," 2000).

The main tool hackers use to create a back door into a system is similar to a toolbox with automated features. The toolbox is referred to as a root kit because it allows the hacker to grow the *roots* of the attack before the visible *tree* pops up. Root kits can create a back door into the system by opening TCP ports through which the hacker can enter the system. When the hacker connects, the root kit becomes a toolbox of malicious programs that can spy on the computer, alter computer files, and even hide the hacker's presence from the network administrators. Root kits have the ability to cloak themselves from the computer and any virus scanner, thus making them a dangerous threat (Szor, 2005). Often, root kits are disguised as legitimate programs to

entice user downloads. The disguised programs are called Trojans (named from the historic Trojan horse) and will be discussed later in this section.

Social Engineering and Non-Direct Attacks

Apart from trying to break into the computer itself, hackers can attempt to affect computer users by interacting with them or altering their connections to different hosts. Users also can be affected by an indirect attack such as a virus. Virus attacks are undesirable to receive.

Phishing. The computer world's users are like a pond of fish with which a hacker may use to go *phishing* for someone who is willing to take the bait. Phishing occurs when a hacker assumes the identity of a company or person of interest and attempts to trick users into providing sensitive information. In most phishing incidents, the hacker creates a false website that very closely mimics a real company's website. The false website is completely functional with the same links that the real website contains, but the false website reports all of the information that a user enters into its forms to the hacker. Once the website is ready, the hacker sends out false e-mails to users attempting to lure them to the fake site. Most phishing attempts use very general phrases (such as *Dear customer)* and other phrases that lack information that the company should know (Panko, 2007). However, some of the cleverer phishing attempts are done by the hacker obtaining customer information through various methods including those mentioned in this paper. Most luring e-mails request immediate action and invoke strong emotion in the readers to cloud their judgment ("Phishing, 2006"). The email then links to the fake site and requests login information and usually personal information such as bank/credit card numbers, social security numbers, etc. All of this information is then recorded on the hacker's server while the user is thanked for cooperating.

Obviously, a company would not want to become a target of phishing. Phishing encounters can make customers feel uneasy using the company's website resulting in a damaged company reputation. The company also must deal with identity theft issues concerning its customers. In order to avoid these misfortunes, companies should have clear warnings about phishing attempts and as they watch for and educate their customers about questionable types of e-mails ("Phishing, 2006").

Spoofing. A similar attack to phishing is called spoofing. Spoofing is done by creating a fake website and forcing a user to go there ("Common Types of," 2008). A common form of spoofing is DNS spoofing. As previously stated, a DNS server translates a domain name (such as www.google.com) into the IP address for the website server. The DNS server does not have enough space to store the IP information for every website on the web, so it usually has to ask other DNS servers for the information requested by the user. The DNS server then stores the information in its cache, which is its temporary storage (Felten, Balfanz, Dean, & Wallach, 1997).

A DNS spoof can occur when a DNS server is programmed by a hacker with incorrect information that usually leads to a website controlled by the hacker. The hacker will ask the victim's DNS server for an IP address that is stored on only the hacked DNS server. The DNS server will have to ask the hacker's DNS server for the requested IP address in order to answer the hacker's request. The hacker's DNS server is programmed to send all of its programmed false IP addresses along with the requested IP address. The incorrect IP addresses will then enter the cache to *poison* it until the next update. At this point, if part of the incorrect information states that www.google.com has the IP address of the hacker's website, then when the victim

tries to visit Google's website, the victim will actually be taken to the hacker's website (Felten, Balfanz, Dean, & Wallach, 1997).

For less technical explanation of DNS spoofing, imagine a driver trying to follow a set of instructions to reach a destination. At one point, the instructions become convoluted and the driver must ask a pedestrian for clarification. The pedestrian has bad intentions and updates the instructions to lead the driver to a gang-controlled territory. Not knowing any better, the driver follows the instructions and ends up in the wrong place. After backtracking a bit, the driver asks someone else for instructions and is given correct instructions. The same process works with DNS spoofing. Once a DNS server updates its cache with correct instructions, it is no longer *poisoned.* The trick is to realize that one is in the wrong place. Realizing this trick can be difficult when the DNS spoof routes to a spoofed website.

A web spoof is very similar to phishing, except it is a less direct attack. Apart from a DNS spoof taking the user to a spoofed website, a hacker also can associate commonly mistyped domain names to a spoofed website. For instance, if one were to enter www.goohle.com, it is possible that a hacker can spoof the Google page so that the user will use it instead of the real page. Just like with phishing, spoofed websites can record everything that the user enters. Whenever a user attempts to go to another website from the spoofed website, the hacker's server can download the outside website so that the user can continue using a spoofed website. The hacker also can change the data that a user sends over a spoofed website such as the shipping address. Ultimately, the hacker can spoof the entire Web for the victim which can be very devastating if the user visits sites with logins and other important data (Felten, Balfanz, Dean, & Wallach, 1997).

Denial of service. When driving home after work during rush hour, one may find that the interstate is often so crowded that no cars are able to move. The traffic jam is similar to a denial of service (DoS) attack. The purpose of a DoS attack is to overload a system with information so that one or more people cannot use it ("Common Types of," 2008). Sending large amounts of data through the system, logging on too many times, or filling up the hard drives with data can all cause a system to not be able to function. DoS attacks can be used to cause general chaos or to crash programs, which, as explained by buffer overflows, can open a way for hackers to break into the system ("Network Security", 2000).

Viruses. Viruses are nuisances that almost every computer user has dealt with at some point. A virus is a program that, much like a real virus, exists for the sole purpose of replicating itself. Unfortunately, the replication process involves a bit more than a simple copy and paste maneuver because viruses require hosts to infect. In this case, the host is any computer file that the virus can find. When the virus copies itself to a file, the file often become corrupt because the virus adds data either before, after, or inside the program's code which makes the computer not be able to use it anymore. Since it takes time for a virus to propagate, infected computers will become increasingly more unstable instead of simply failing the instant a virus arrives. Once the virus completes its task, it typically tries to transfer to a different computer via the network (Paquette, 2000).

A special type of virus that is particularly troublesome for networks is a worm. A worm *tunnels* its way through a network in order to infect as many computers as possible. Unlike most normal viruses which need the user to activate them, worms are automated, which makes them even more deadly. Often, worms will travel over e-mail. Once a computer is infected, the worm

attempts to read the user's address book and send a copy of itself to everyone on the list, which classifies them as mass mailers (Szor, 2005).

Trojans. Trojans are special tools that a hacker uses to infiltrate a system. They are particularly dangerous because they hide within useful programs. Take for instance a free game that one might find online. Once downloaded, the game may launch and play as the user would expect, but behind the scenes, the program launches a hidden Trojan that makes its way into the system. From there, the Trojan can do a multitude of things including downloading other malicious files, spying on user activities, and create back doors into the system. What is worse is that Trojans are particularly good at hiding from virus scanners and it is often difficult to clean the system of them (Szor, 2005).

Spyware. As if viruses and Trojans were not enough to worry about from hackers and irate programmers, actual companies attempt to plant spyware on user computers. Spyware, as the name suggests, is spying software that is used to collect data on user activities and report them back to the company. Some spyware programs are designed to hide from the system and silently collect data, while others are made to throw continuous pop-up advertisements at the user ("Impact of Spyware, 2006). Either way, spyware that is allowed to remain on a computer typically starts to slow down the system until it becomes unusable.

A good amount of the spyware circulating on the Web uses a similar technique to the Trojan in that spyware is often hidden within software. In some cases, removing the spyware will cause the program it came with to stop functioning as per its instructions. Also, using a provided uninstall program usually removes only the visible spyware while leaving the actual spyware on the computer. The manual removal of spyware also poses a problem in that if the entire spyware set is not removed, its components can re-download the missing parts. It is very difficult to

remove all of the spyware parts since many spyware files are deeply hidden in the system ("Impact of Spyware", 2006).

Man-in-the-middle and hijacking. The man-in-the-middle is a phrase used to refer to a hacker who interrupts a connection between two computers ("Common Types of," 2008). Once the connection is intercepted, the hacker can then monitor the communication between the computers as well as alter the data that is sent. Similarly, hijacking involves the hacker rerouting the connection to one of the computers so that the other computer communicates with the hacker's computer. Then, the hacker can send and receive anything to and from the other computer ("Network Security", 2000). Based on the information provided in this paper thus far, one can only imagine what things may be sent at that point.

Sniffers. A sniffer is a special tool that allows a user to track different aspects of the network such as network traffic, sent data, e-mail content, etc ("Common Types of," 2008). Sniffers are actually security tools for network administrators to use in order to ensure that no one is trying to break into the network and to ensure that network users are behaving themselves. As one would expect, however, hackers are more than happy to turn these tools against the network for their own gain. With sniffers, hackers can see what is sent over the network and the internet as well as copy any unencrypted information with little to no effort (Andrés & Kenyon, 2004).

Given the amount of damage that they can cause, network threats are necessary to prevent in order to run a business or own a computer. Although never falling victim to an attack is unlikely, a company or user is safer when employing protective measures to lower the chances of becoming an attack victim. The next section will describe several different types of network security measures.

Components of Network Security

Due to the constant evolution of network threats, network security is a challenge to maintain both for network administrators and the companies that produce network security products. As many security experts have proclaimed, the only truly safe computer is a computer that is never plugged in and kept locked up in a safe for the duration of its existence ("Network Security", 2000). Since such treatment of a computer would render it useless, users are forced to submit the machine to the risk of attack. To protect a computer from the many network threats, users can employ a variety of methods (e.g. controlling access to a network/computer, monitoring the network, and employing attack prevention measures).

Access Control

Authentication. A common theme in the security portion of this paper has been authentication – mainly by use of passwords. Authentication can, however, consist of other components than passwords. Authentication is based on four principles: *what you know*, *what you have*, *who you are*, *and where you* are ("Network Security", 2000). Each of these principles can be used individually or in conjunction with one or more other principles.

The *what you know* principle most directly relates to the user being able to provide a username and password in order to access a system. The *what you know* authentication principle relies on a person's knowledge to grant or deny them access to the system. Of course, the *what you know* principle is useful for only as long as the relied upon knowledge is kept secret from illegitimate users. Hence, using this principle alone is not usually a safe way to protect a network (Innella, 2001).

The *what you have* principle is somewhat difficult to apply to securing a computer because it deals with physical possessions. For example, an access card that must be scanned to

open a door is an example of this principle. Although most computers do not usually have a device that requires a physical authentication method, many companies use leveled access cards to prevent unauthorized users from accessing certain rooms such as server rooms. Of course, this authentication method is useful only as long as the necessary physical identification device is not obtained by an unauthorized person ("Network Security", 2000).

The *who you are* principle deals with the unique physical characteristics of a person such as fingerprints, retinal scans, and voice recognition. Some personal computers such as laptops employ this principle in place of a password for both convenience and extra security for the user. The *who you are* authentication method both cannot be replicated or guessed like a password and cannot be shared or stolen by other people ("Network Security", 2000).

The *where you are* principle deals with a computer's geographic location. The *where you are* principle can use a computer's IP address to determine where the computer is located and determine whether the computer is in an authorized zone. Of course, since IP addresses can be spoofed, proxied, and hidden by NAT, the *where you are* principle is not a good authentication method to use by itself. By combining this principle with other principles, it can prove to be very powerful, especially if an unsuspecting hacker attempts to use a stolen password from an unauthorized location ("Network Security", 2000).

Key management servers (Kerberos). Another secure authentication method is the Kerberos server which acts as a gatekeeper between two computers. The Kerberos server is a protocol that uses special encryption keys to verify a user's identity. In order for two users to connect to each other, they must both have the specified keys to authenticate with the Kerberos server. The server then provides the users with a special key to encrypt data during their connection. By using encryption, users can send data to each other without worrying about

hackers stealing their data ("Kerberos," 2007). Encryption will be discussed in more detail later in the paper.

The Kerberos server is able to provide an authentication method with data encryption and integrity. Since the server is able to authenticate users on their own computers, no authentication data is sent over the Internet which means that hackers cannot intercept any sensitive data. On the downside, if the server becomes compromised by a hacker, any data sent over it also is compromised. Also, the server cannot ensure that the connecting clients are secure from other threats such as viruses. Lastly, if a user fails to close their connection to the server, other users can access the server without needing authentication ("Network Security", 2000).

One-time passwords. A special type of password is a one-time password that, as the name suggests, can be used only once. Servers using one-time passwords contain a list of passwords that it uses to reference the current authorized password. An example of a one-time password's usage is to require users to enter their normal password with the minute of their login added to the end of the password. Thus, if a hacker intercepts the password, they would have to determine that the last two numbers corresponded to the minute of the logon and alter the password to login ("Network Security", 2000). The chance of a hacker guessing the one-time password scheme is unlikely if a scheme is developed well.

Access control list. Once a user becomes authenticated by providing the required credentials, a system can use the authentication to determine which files the user can access. An access control list allows for this selection method. System administrators can group each user within different access levels in order to grant or restrict access to certain data. Besides controlling access, administrators also can define how users can interact with files. For example, a file can be made read-only which means that a user can only open the file to view its contents,

but the user cannot make any changes to the file. Conversely, a file can be write-only which means that a user can only add to the file, but not view the contents of the file. Only users with the necessary rights to change these file settings can use the file in a different way than specified ("Network Security", 2000).

Execution control list. Whereas an access control list can restrict user access to files, an execution control list can restrict user access to program functions. For example, Microsoft Windows provides the ability to change the date and time settings for the system, but there is no reason for a company user to do so. Therefore, a company may choose to block that function for its users. Execution control also can be used on simpler programs such as internet browsers to prevent unsafe changes to the program's settings. Execution control can help prevent employees from damaging the system by changing settings haphazardly as well as help keep employees within the allowed areas of the computer ("Network Security", 2000).

Network Monitoring

Apart from controlling network access, network administrators also must be aware of what is going through their networks. The way to achieve this knowledge is by monitoring the network traffic. Monitoring traffic can be a tedious task, so most administrators use tools to assist them.

Intrusion detection system. Although it is preferable to prevent an attack so that it does not occur, such luck is not always available for companies. In the case that an attack succeeds, employing an Intrusion Detection System (IDS) can help minimize the consequences to the network. An IDS helps to analyze the network logs that are created by firewalls in reference to network activity (McHugh, Christie, & Allen, 2000). Such logs are generated for each connection which often means that there can be several thousand per day to audit. Without an

IDS to assist the auditing process, a network administrator would need to view every log manually in order to implement good security practices for the company (Sundaram, 1996). An IDS also will check the network traffic based on a predefined profile that depicts the typical usage of the network. If it detects either a questionable log or a strange connection, it will alert the network administrators that there is an attack on the network so that they may take action (Marin, 2005).

An IDS also can detect strange patterns from a network connection. Abnormal behaviors also are compared to a predefined profile that prototypes normal network behavior. For example, if everyone in a secure building is supposed to wear a dark green coat and a top hat and a guard sees someone who is wearing a light green coat and a ball cap, the non-conforming individual will be flagged as an intruder. Unfortunately, the strange behaviors on a network are a lot more difficult to determine than simply visually picking something out of the crowd. Therefore, a poorly configured IDS can often point out normal traffic as bad or miss actual bad traffic (Sundaram, 1996). Therefore, the IDS profiles must be updated regularly to accurately portray normal network usage. Despite all of the extra trouble to keep an IDS functioning, companies are much better off knowing when an attack has occurred instead of possibly not finding out until much later (McHugh, Christie, & Allen, 2000).

Network utilization. Network utilization is mainly used within a locally managed network. Network utilization monitors how much data is transferred to and from each computer. Each user will have a shared average amount of data transferred from their computers. If a particular user consistently uses more network resources than others, that user may be conducting unsolicited activities ("Security Auditing, Attacks," 2000). Although the user in question may just be doing more network-intensive work than others, in the case that the user is participating in unsolicited

activities, that user may cause a denial of service for other employees since the network resources are being used too much by one person (Noonan, 2004).

Network analyzer. Network analyzers are able to determine the origins, content, and destinations of network messages (Marin, 2005). The previously mentioned sniffers are an example of a network analyzer. If a user is suspected to be performing unsolicited activities, a network analyzer can quickly and silently tell administrators whether their suspicions were correct. Network analyzers also can be used to determine where an attack came from by providing such information as an IP address (Noonan, 2004).

Network reports. Network reports, which also include the aforementioned network logs, can help provide important information about past network transmissions. Network reports can provide clues as to where a connection originated and what system(s) may have been affected by an attack. Reports also can help determine how an attack got through the security as well as when it got through. By reviewing these reports, administrators also can determine the weak points in the network's security and how to modify the security policy to prevent a similar attack from occurring again ("Security Auditing, Attacks," 2000).

Attack Deferral

As previously stated, it is preferable to prevent an attack from happening instead of having to deal with one. The best way to prevent an attack is to make it more difficult for a hacker to break in a system. Such methods are used by implementing tactics to either stop an attempted attack or distract a hacker while administrators can respond to the attack.

Firewalls. Perhaps the most well recognized term in network security; firewalls are understood to be a necessary part of any computer. Unfortunately, many common users regard the firewall simply as *that thing that stops me from using program x or y*, which causes casual

users to under-value the purpose of a firewall. The term *firewall* originates from a reinforced door that comes down to stop the spread of flames in a building, but a firewall actually functions more like the biological wall of a cell in that it is semi-permeable (selective about what gets through) based on its instructions.

A firewall is used to keep intruders out of the network and to prevent certain information from exiting the network based on a set of rules. The rules of a firewall should reflect what is and is not acceptable for the use of the network. By blocking or allowing traffic appropriately, network administrators can help enforce a secure network environment (Noonan, 2004).

As many company employees are well aware, firewalls also are used to prevent users from accessing certain areas of the Web. Apart from trying to keep users on task, blocking these services also functions to prevent company information from being sent to unsolicited people. As mentioned earlier, Trojans will often collect and send data to their programmer. By properly implementing a firewall, companies can be safe from most of these types of threats since they will block data being sent over abnormal ports. Also, in some cases, an employee may attempt to send someone a company file or password over an unsecured program such as an instant messenger that could be easily intercepted by a hacker. Some malicious employees also may try to send company information through personal programs to avoid company detection. Both of these issues can be prevented by blocking these services with a firewall (Andrés & Kenyon, 2004).

Many firewalls use a method called packet filtering to block bad traffic. Firewalls use a set of rules defined by administrators to determine if a packet is acceptable. Firewalls using packet filtering inspect the packets entering the network in order to keep the network safe ("Network Security," 2000). Simply stopping incoming traffic is often not enough to keep a

company secure. Therefore, many firewalls also filter outgoing traffic to prevent certain programs from working and to prevent things like Trojans from sending data to outside sources.

Firewalls can control access to a network in two ways: to allow access to certain traffic and to deny access to certain traffic (Andrés & Kenyon, 2004). The selection of which method to use can completely change the way that a firewall must be setup. When allowing access to certain traffic, a firewall is initially set to block all traffic. The network administrators will then program rules for the firewall to follow in order to allow certain access to necessary programs and websites. When denying access to certain traffic, a firewall is initially set to allow all traffic. The network administrators will then program rules for the firewall to follow in order to block certain access to undesired programs and websites. Most companies have their firewall block all but certain traffic in order to make the firewall easier to program.

Apart from blocking traffic, firewalls also provide other security features. A common feature provided by both firewalls and routers is called Network Address Translation (NAT). NAT will give the firewall or router a single IP address that is shared by the entire network (Panko, 2007). All of the traffic going in and coming out of the network will use the same IP address, while the computers within the network will each have a local IP address. Local IP addresses, commonly seen as a 192.168.x.x address, are replicated across several networks. The NAT device will translate the local address into the shared address and vice versa. Therefore, any hacker who attacks the shared IP address will attack only the NAT device which is usually the firewall. Such attacks are usually fruitless (Andrés & Kenyon, 2004).

Another special feature a firewall can provide is to create a DeMilitarized Zone (DMZ). A DMZ's function is to separate a company's public network from its private network. In other words, a DMZ separates public servers from private servers and computers. With a DMZ, if a

public server gets attacked, that server will not be able to affect the other computers on the network because the DMZ will block any connections from that computer (Noonan, 2004). Thus, a company can maintain a public server for outside users to access while simultaneously keeping the rest of their network safe. The disadvantage to a DMZ is that any computer within its zone is much less protected from attacks.

A special type of function of some firewalls is to provide a proxy server. Most users who have snooped around in their internet browser settings have probably noticed a section about proxies. A proxy is a special server that acts as an agent for other computers on the Web. Each computer will ask the proxy server to obtain or send information on the Internet and the proxy will obtain or transmit this information for them. By using a proxy, the user computers do not transmit their IP address to the webservers to which they are communicating. Instead, the proxy server's IP address will be sent to the webservers. Proxy servers also can be based off-site of the company or user's premises. The main point of a proxy is to hide network information from hackers so that they cannot trace a connection. The process is similar to a *Don't shoot the messenger* concept ("Network Security", 2000).

Intrusion prevention systems. Unfortunately, firewalls alone cannot keep a network safe from attack. To further protect a network, a company may employ an Intrusion Prevention System (IPS) to monitor and control traffic in the network. Two types of IPS may be employed at a company: a Host IPS (HIPS) and a Network IPS (NIPS) ("Intrusion Prevention Systems," 2004). As their names suggest, HIPS deals with a single computer while NIPS deals with the whole network.

The Host Intrusion Detection System works to prevent attacks from occurring on a single system. Its main function is to monitor the system operating files and prevent unauthorized

changes to them. The HIPS also monitors other programs and their settings to ensure that each program will stay operational. Finally the HIPS will monitor network traffic coming to and leaving that computer to make sure that it is authorized, and it will keep logs of all system activity for later auditing. The main problems with a HIPS is that it may slow down the computer's speed, it may block legitimate network traffic, and it may not work with operating system upgrades since the HIPS works so closely with the operating system ("Intrusion Prevention Systems," 2004).

The Network Intrusion Prevention System differs from the HIPS mainly because it has a firewall. NIPS firewalls are slightly more advanced than most normal firewalls in that they have the ability to detect and cut off connections with bad data. Most common firewalls will simply attempt to close the connection with the sending computer which usually takes more than enough time for malicious data to travel through the network. The NIPS will simply block all of the data proceeding the malicious packet. The difference between a NIPS firewall and a normal firewall is like slamming the door in a salesperson's face versus telling him *No thank you* and waiting for him to leave. The NIPS also will facilitate the flow of legitimate data by reorganizing the packets that it inspects so that the receiving computers can interpret the data easier ("Intrusion Prevention Systems," 2004).

Virus scanners. Although virus scanners are commonly used to disinfect a computer from viruses, the ideal use of a virus scanner is to prevent a computer from being infected in the first place. In order to prevent infection, a virus scanner must be able to quickly and effectively scan everything that enters the system. Most virus scanners use a real-time scan function to analyze each file as it is accessed by the computer or user. Real-time scans in conjunction with frequent

full-system scans can help keep a computer free of viruses to both prevent system damage and keep back doors closed to hackers.

Virus scanners use a variety of methods to scan for viruses. String scanning, generic detection, and filtering will be discussed as examples to explain how virus scanners work. String scanning searches for program codes that are not typical for normal programs (Szor, 2005). For example, if one were to type *infromation* in a program with spell checking capabilities, the program would point out that the word is not spelled like a normal word. Also, string scanning references known virus codes from a database in order to locate a virus. Using the *infromation* example, if a program with auto-correction capabilities finds the misspelling, it will likely replace the word with *information* since its database lists the misspelling and how to deal with it. Unfortunately, like with some misspelled words being auto-corrected with an incorrect word, virus scanners can often disinfect a file incorrectly which would break the file. File damage is caused by a scanner removing a variant of the detected virus without recognizing that it is a variant. System administrators must therefore configure the virus scanner to make a backup of each file that it disinfects so that it can be restored if needed.

Generic detection is used to help detect virus variants. Generic detection uses wildcards to skip over certain variable code so that any variations of the virus cannot avoid detection (Szor, 2005). If, for example, a person was trying to find a four letter word beginning with *f* and ending with *d*, the person could use wildcards to hold the place of the unknown letters to display *f_ _d*. A search for this string of text could result in food, feed, fled, etc. Virus scanners use generic detection to find virus variants in the same way. Since certain parts of the code will be the same for each virus, wildcards can be used to ignore the variable parts. Generic detection also is faster

than string detection because it is able to search for variants with a single string search instead of one string for each variant.

Commonly, filtering is used for quick scans and real-time scans. For example, if there is a sweepstakes and only bags of barbeque potato chips may contain the winning number, participants will filter the other chips and look strictly at the barbeque chips. Scan filtering works the same way. If only .exe files can contain Virus A, then the scanner will not scan other types of files for that virus. Filtering is made possible since some viruses require certain types of files to spread. By using filtering, virus scanners can drastically speed up the scanning process since they no longer need to scan every file for every virus (Szor, 2005).

Encryption. Encryption is a powerful tool for secure data transfers. Its main function is to scramble text based on a key. Keys are a string of text, much like a password, that a computer enters into a complex mathematical equation to generate a method to encrypt a block of text. Once the text is encrypted, the information can no longer be interpreted by anything unless the decryption key is discovered (Panko, 2007). For example, encrypting the text, *How are you?* may appear as, *hE5C5Dcp)E&u*, which is incomprehensible to a person unless it can be decrypted back into its original form. The key is like an answer key to a scan-able test form. Without the key, the machine has no way of knowing whether the information presented to it is correct or not.

Encryption uses rounds to encrypt data. A round, as the name suggests, is a single pass over the data. Most encryption methods use several rounds to encode the data. With each round, the text becomes less like its original state so that it cannot be deciphered easily by someone without the key ("Network Security," 2000). Imagine passing a marshmallow over a flame while taking a video of the process. With each pass, the marshmallow will become more and more

misshapen until it is almost undistinguishable by its original form. The decryption method for the marshmallow would be to use a machine that can rewind the video until the marshmallow is in its original form. As one can assume, the more rounds that encryption makes, the more secure the data is while also taking a lot more time to encrypt and decrypt the data.

An example of an encryption method is symmetric-key encryption. symmetric-key encryption uses a single key to both encrypt and decrypt the data ("Network Security," 2000). As one might expect, both parties must be in possession of the key in order to make this method possible. The trick behind symmetric-key encryption is how to send the key to the other party. E-mail is an ideal way to send a key, but since e-mail is so unsecure, the data may as well not be encrypted. The best way to transmit a key is to do so in-person, but then again, personal meetings are not always possible. In order to circumvent the necessity to transmit a key, a new form of encryption was implemented.

Asymmetric-key encryption allows for a key to be kept secret from anyone else since one key is used to encrypt data and another key is used to decrypt the data. In asymmetric-key encryption, one key is made available to the public on the Internet so that anyone can use the key to encrypt the data and send it to the public key owner. Since the other key is kept on the owner's computer and never sent, the key cannot be stolen unless a hacker breaks into the computer itself and finds the key. Asymmetric-key encryption uses highly intense mathematical equations to encrypt data while making it impossible to decrypt without the other key. While this method is very secure, the intense math makes this method take a very long time to encrypt data; often a few hours for a small amount of data ("Network Security," 2000).

Another form of encryption uses something called hash code. Hash code is a special form of the encrypted data that can never be decrypted by anything. The purpose of hash code is not to

be interpreted, but to be compared. Think of a product that has a label on it that reads, *If this label is broken, do not buy*. The label is similar to hash code in that if any change to the file has been made, the hash code also will change. Therefore, hash code coupled with an encrypted file when it is sent can be compared with the hash code of that file when it is received to ensure that no one attempted to alter the file while in transit. Encryption is both useful and necessary for secure data transfer ("Network Security", 2000).

Honeynets. Imagine that a bear is a hacker. In order to keep the bear away, network administrators will set up jars of honey to distract the bear so that the administrators can react to the bear's presence without actually facing the bear head-on. A honeynet does exactly that. It is a false network setup to trick hackers into breaking into it. The honeynet usually appears to be a weak-point in the network so that hackers will be more likely to try breaking into it. If a user begins sending messages to a honeynet, there is a very likely chance that the user is intending to cause harm. Honeynets allow administrators time to react to an attack while also protecting the real network from attack. Therefore, administrators will not have to scrutinize innocent users performing normal business as strictly (Andrés & Kenyon, 2004).

Companies and computer users often invest in security measures in hopes that they will be safe from an attack. Although preventative measures do not always work, most security measures provide monitoring and recovery options so that administrators can respond to threats. Apart from using security hardware and software, users must realize that security is not limited to technology. Hypothetically, even the safest network is subject to attack if its users are not conscientious about what they do on the computer (Harrison, 2005). Therefore, companies must create a security policy to enforce proper employee conduct on its computers.

Creating a Security Policy

Having a security policy is yet another powerful tool that can help protect a network. By itself, the policy cannot actually fend off attackers, yet it can tell the people within a company how to act, how not to act, and how to respond to attacks. Both administrators and users have responsibilities in a security policy. Upholding these responsibilities is the only way to make a security policy effective (Jarmon, 2002). The security policy also should include how administrators should deal with security breaches.

Administrative Responsibilities

Defining acceptable activities. The first thing an employee is told on his/her first day is what to do on the job. A security policy also should include what an employee should do on a computer. A simple way to begin describing what to do with company computers is to define how the network should be used. Defining the reason that the network exists and what users are expected to do while on the network can clear up any of the incorrect assumptions that a deviant user may decide to make (Jarmon, 2002). Apart from the general network, a security policy should describe what programs are available for the job and how they should be used. Security policies should list the types of programs that are allowed on the computer so that users will not install unsafe or illegal software. Lastly, the policy should describe what types of websites are permissible to visit on the company network ("Network Security", 2000).

Defining unacceptable activities. Although most administrators would hope that a list of acceptable activities would make what is unacceptable obvious to users, simply defining acceptable activities can be too vague to effectively prevent unauthorized actions. It is therefore necessary to include a list of unacceptable activities within a security policy. The first items of the list should define how the network should not be used ("Define a Network," 2008).

Downloading programs, file sharing, and testing downloaded programs on company computers are a few examples of such activities. Specifying the types of websites also can prove necessary. Questionable sites such as those which offer free downloads, pornographic sites which can offend others and sneak viruses onto computers, and sites that could cause liability to a company are examples of sites that should be specified as unacceptable. Administrators also must define the penalties for disregarding the rules so to defer users from breaking them ("Network Security", 2000).

E-mail content security. Since e-mail is so easy to intercept and attack, administrators also must define how to use the e-mail system. Many companies choose to restrict non-business e-mails from being sent to a company e-mail address, which helps to cut down on the receipt of spam and denial of service due to having too many e-mails ("Define a Network," 2008). Security policies also must specify what type of information must not be sent over e-mail such as credit card numbers, passwords, encryption keys, etc. since the messages can easily be intercepted by hackers. The types of e-mail attachments also must be limited since viruses can exist within certain files.

Apart from simply defining what not to do, administrators also should mention how to avoid issues. If an employee receives an e-mail from an unknown sender, the message should be heavily scrutinized and potentially not even opened just in case there is a threat present. Users also should be warned to be wary of strange attachments that could potentially contain threats (Jarmon, 2002). Users also should be prompted to immediately delete spam since clicking the ever-so-tempting unsubscribe link often signs the user up for more spam instead of unsubscribing their address.

An e-mail policy also should include procedures as to how to secure data. The policy should describe what kinds of data need to be encrypted and how to encrypt it ("Define a Network," 2008). Also, a detailed procedure describing how to transfer the encryption key to the other party should be made. Finally, there should be a note about what types of data not to list or request in an e-mail so that no sensitive information can be stolen (Singapore, 2002).

Educate users. Apart from listing the do's and do not's in the security policy, a company also may choose to include the why's as well. Users will often be less resentful of the rules if a description of why they exist is available. Many companies also try to educate its employees about the threats on the Internet so that they will be able to use the computer more cautiously (Jarmon, 2002). Teaching users about how to take a proactive approach to network security also can help to prevent problems. For example, teaching users to save and scan an e-mail attachment can help catch threats much better than crossing fingers and opening files directly. Users also must know what to do when there is a security issue present. Reporting possible issues, not simply hoping a problem will go away, and not solving problems alone can help prevent disasters (Singapore, 2002).

User Responsibilities

Network users have a much easier job than the administrators: follow the security policy. Following the acceptable and unacceptable use policies can easily prevent network catastrophes. Users also must keep their secret information away from others so that no one other than the individual person can access their authorized systems. Users also can assist network security by understanding the threats on the network and how to respond to them (Jarmon, 2002). Even if a user is skilled at using a computer, the best course of action for them to take is to follow the

security policy's instructions of how to respond to a threat. By following the policy, a user who knows less than assumed cannot damage the system (Singapore, 2002).

Disaster Response

Apart from describing how a user should respond to a problem, a security policy also should explain administrators' responses to an attack. The policy should include the preemptive stages of risk management and network monitoring as well as an attack response plan and how to evaluate the entire policy.

Risk assessment. With so many separate components in a network, administrators have a difficult task to determine which components are vulnerable. The network must be tested by network employees to find security flaws by pretending to hack into the network. Network tests will show where the security's weaknesses lie. Administrators also must remain updated about the bugs and exploits of all of the software that is available at the company (Jarmon, 2002). Awareness and knowledge will help administrators watch for potential attacks or determine if having a program is worth the risk. Program updates also must be tested to ensure that the new versions do not contain bugs that will make the network vulnerable ("Network Security", 2000).

Often, detected risks are expensive to secure. Therefore, administrators must take care to balance the risk with the cost in order to determine which risks to remove first. Certain risks may be more likely to be exploited while other risks may be easier to fix (Singapore, 2002). In some cases, a dangerous risk may be left open for a long time since fixing it would involve a long network downtime. Therefore, risks must be weighed against several factors (such as which assets generate more revenue) to determine which risks to fix first. Either way, the long-term goal of a networking department is to remove all risks eventually (Jarmon, 2002).

Monitoring policies. Even the network administrators can try getting in trouble with the power they have. Although monitoring a network can help detect attacks, monitoring transmissions too deeply also can be an invasion of privacy. Administrators must therefore be kept in check by the security policy. The policy should determine what kind of network traffic to monitor as well as how deeply to monitor the traffic ("Define a Network," 2008). For instance, the policy should state that the actual data cannot be viewed unless it comes from a strange IP address. The policy also should state who is authorized to monitor network transmissions.

In the case of employee misuse, the policy should include how administrators should deal with the infraction. Some companies may choose to issue warnings. In such a case, the policy should state how many warnings a user should receive before harsher action is taken. Other companies may choose to take harsh action upon the first offense. The policy should include such punishments as well. By listing the punishments, the company cannot step out of line when responding to an infraction and the user can be well aware of the consequences for unauthorized actions (Singapore, 2002).

Attack response plan. When disaster strikes, administrators need to know how to deal with the problem. The security policy should state what services need to be protected first and how to protect them (Jarmon, 2002). Administrators should have a way to inform employees about the problem so that they will not transmit sensitive information while the network is compromised. Administrators should be familiar with these policies well before any attack occurs so that they will not need a reference during a moment of crisis.

Apart from defining how to respond to an attack, the security policy also should define how to recover from an attack. Policies about how to check for damage to the network computers, how to discover what was stolen, and how to check for altered files should be made. One of the

most useful methods to recover from an attack is to use backups. A security policy should specify how often and where to backup data. The policy also should specify how long to keep an archived backup to use in case a later backup was attacked or infected by a virus. The policy also should include the procedures to restore a backup to a damaged system so that the damage will not remain on the system after the backup is applied (Singapore, 2002).

Evaluation. The one good thing to gain from an attack is a lesson. In order to learn a lesson from an attack, the security policy should detail how to evaluate the policy's effectiveness. Being able to determine where a policy failed can help strengthen the policy to prevent the same thing from happening again. For example, if an unblocked unnecessary service was the cause of the attack, the policy should be updated to block that service (Jarmon, 2002). Administrators also must evaluate their response to an attack to determine whether they were adequately prepared to defend the network. Evaluating the backup system is also an important step to ensure a quick recovery.

A security policy is never a finished product, as it must be updated constantly in order for a company network to stay well protected since network threats are always changing. The policy must be thorough and specific so that company users can understand how to behave on the company network. Policies must be well written, as a poorly written or overly strict security policy can hurt the company's flow of business. Lastly, the security policy should work with the security hardware and software to ensure network security as best as possible.

Conclusion

Although the Internet is full of threats, its users can stay safe by knowing how to avoid calamities. Even though attacks from hackers are difficult to avoid, most home users can surf the Web without falling victim to viruses and spyware as long as they are wary of what websites and files to avoid. The trick is to actually learn how to avoid threats on the network. In order to do so, users must stay informed with the latest information by constantly researching and altering their computer usage. Otherwise, they can lose their data or even their identity to a crafty attack.

Businesses must keep a keen eye out for strange network behavior. Even though most attacks come from outside of the company, problems can still originate from inside the company. Network administrators must know how to properly configure their network resources to block and log any activities that may attempt to hurt the company. They also must create and enforce a well-written security policy and keep it updated to close security gaps. Only by remaining vigilant can both network administrators and computer users remain protected from and ready for a network attack.

The information presented in the paper is intended to increase awareness of the threats and security measures on computer networks so that users can learn to better identify network threats and how to deal with them appropriately. The information in this paper should be shared with family, friends, colleagues, employees, etc. to help increase security. If someone on a network is affected by a security breach, that single incident easily can spread to the rest of the network.

References

Andrés, S., & Kenyon, B. (2004). *Security Sage's Guide to Hardening the Network Infrastructure*. Rockland, MA: Syngress Publishing, Inc.

Boswell, B. (2003). Preventing Spam in a Windows Environment. *Windows Consulting Group, Inc*. Retrieved April 19, 2008, from download.101com.com/techlibrary/mcafee/prevent_spam_mcafee.pdf

Buffer Overflow. (2005). *McAfee System Protection Solutions*. Retrieved April 4, 2008, from www.mcafee.com/us/local_content/white_papers/wp_ricochetbriefbuffer.pdf

Common Types of Network Attacks. (2008). *Microsoft TechNet*. Retrieved February 9, 2008, from http://www.microsoft.com/technet/prodtechnol/windows2000serv/reskit/cnet/cndb_ips_ddui.mspx?mfr=true

Define a Network Security Policy. (2008). *Hewlett-Packard Development Company, L.P.* Retrieved February 6, 2008, from http://www.hp.com/sbso/productivity/howto/security/

Farley, M. (2005). Storage Networking Fundamentals: An Introduction to Storage Devices, Subsystems, Applications, Management, and File Systems. Indianapolis, IN: Cisco Press.

Felten, E. W., Balfanz, D., Dean, D., & Wallach, D. S., (1997). Web Spoofing: An Internet Con Game. *Technical Report 540-96.* Princeton University.

Gibson, R. W. (1990). *IEEE Project 802 Standards Efforts*. Retrieved March 10, 2008, from IEEE database.

Harrison, J. V. (2005). *User Malware:* Enhancing Network Security By Preventing User-Initiated Malware Execution. *International Conference on Information Technology: Coding and Computing*, 2, 597-602. Retrieved February 18, 2008, from IEEE database.

The Business Impact of Spyware. (2006). *Trend Micro Incorporated.* Retrieved April 4, 2008, from http://us.trendmicro.com/imperia/md/content/us/pdf/products/smallbusiness/clientservermessagingforsmb/wp03bsspy30_060905us.pdf

Innella, P. (2001). A Brief History of Network Security and the Need for Adherence to the Software Process Model. *Tetrad Digital Integrity*. Retrieved February 12, 2008, from http://www.tdisecurity.com/resources/assets/NetSec.pdf

Internet System Management. (2000). St. Louis, MI: Wave Technologies International, Inc.

Intrusion Prevention Systems. (2004). *The NSS Group Ltd.* Retrieved April 6, 2008, from http://www.nss.co.uk/WhitePapers/intrusion_prevention_systems.htm

Jarmon, D. (2002). A Preparation Guide to Information Security Policies. *The SANS™ Institute*. Retrieved March 10, 2008, from http://www.sans.org/reading_room/whitepapers/policyissues/503.php

Kerberos: The Network Authentication Protocol. (2007). *Massachusetts Institute of Technology*. Retrieved April 19, 2008, from http://web.mit.edu/kerberos/www/

Link Layer and Network Layer Security for Wireless Networks. (2003). *Interlink Network, Inc.* Retrieved April 18, 2008, from http://www.lucidlink.com/media/pdf_autogen/Link_and_Network_Layer_Whitepaper.pdf

Maki, M., Hamada, S., Tokuda, M., Shimoshio, Y., & Kuwabara, N. (2001). Home Information Wiring System Using UTP Cable for IEEE1394 and Ethernet Systems. *Consumer Electronics, IEEE Transactions*, 47(4), 921-927. Retrieved April 19, 2008, from IEEE database.

Marin, G. A. (2005). Network Security Basics. *IEEE Security and Privacy*, 68-72. Retrieved February 29, 2008, from IEEE database.

McAfee, J., & Haynes, C. (1989). Computer Viruses, Worms, Data Diddlers, Killer Programs, and Other Threats to Your System: What They Are, How They work, and How to Defend Your PC, Mac, or Mainframe. New York, NY: St. Martin's Press.

McHugh, J., Christie, A., & Allen, J. (2000). Defending Yourself: The Role of Intrusion Detection Systems. *IEEE Software*. Retrieved February 12, 2008, from www.cert.org/archive/pdf/IEEE_IDS.pdf

Network Security and Firewalls. (2000). St. Louis, MI: Wave Technologies International, Inc.

Noonan, W. J. (2004). Hardening Network Infrastructure. Emeryville, CA: McGraw-Hill/Osborne

Panko, R. R. (2007). *Business Data Networks and Telecommunications* (6th ed.). Upper Saddle River, NJ: Pearson Prentice Hall.

Paquette, J. (2000). A History of Viruses. *Security Focus*. Retrieved February 12, 2008, from http://www.securityfocus.com/infocus/1286

Phishing. (2006). *Trend Micro Incorporated*. Retrieved April 4, 2008, from http://us.trendmicro.com/imperia/md/content/us/pdf/products/smallbusiness/clientservermessagingforsmb/ trendMicro_Phishing.pdf

Security Auditing, Attacks, and Threat Analysis. (2000). St. Louis, MI: Wave Technologies International, Inc.

Singapore IT Security Techno Portal. (2002). How to develop a Network Security Policy. *Singapore IT Security Techno Portal*. Retrieved February 6, 2008, from http://www.blacksheepnetworks.com/security/info/policy/netsec1.htm

Sundaram, A. (1996). An Introduction to Intrusion Detection. *Association for Computing Machinery*. Retrieved April 6, 2008, from www.acm.org/crossroads/xrds2-4/intrus.html

Szor, P. (2005). The Art of Computer Virus Research and Defense. Hagerstown, ML: Phoenix BookTech.

Tang, A., Andrew, L. H., Chiang, M., & Low, S. H. (2008). Transport Layer. *Cornell University*. Retrieved April 18, 2008, from http://people.ece.cornell.edu/atang/pub/08/transport.pdf

Wright, J. (2003). Detecting *Wireless LAN MAC Address Spoofing*. Providence, RI: Polarcove.

Appendix

Quick-Reference List

The following is a quick-reference to the topics covered in this paper:

Nine network elements - applications, servers, clients, routers, switches, wireless access points, access lines, trunk lines, messages

Hybrid TCP/IP-OSI - physical, data link, internet, transport, application

Spam - unsolicited commercial e-mails

Brute-force - often automated attempt to guess a password by using all possible characters

Bugs - flaws in a software program that allows illegal access

Phishing - an attempt to steal personal information given voluntarily

Spoofing - an authentic-looking false website

Denial of service - preventing one or more users from accessing a system by flooding it with requests for data

Virus - a self-replicating program that destroys data

Trojans - a functional program that carries a hidden virus

Spyware - a company-made program that reports computer activities and displays advertisements

Hijacking - taking over a connection in place of another

Sniffer - a network utilization monitoring program that also can be used to steal data

Authentication - a method to determine valid users to grant or deny system access

Access control list - a set of rules that determines who can use a particular service

Execution control list - a set of rules that determines what a user can do with a particular service

Intrusion detection system - a system that detects and reports an intrusion in real-time

Firewall - a system that allows or blocks network data based on a set of rules

Intrusion prevention system - a system that prevents network attacks by blocking dangerous connections

Virus scanner - a program that detects and removes viruses by searching for known and likely viruses

Encryption - a process that scrambles messages to make them unreadable by those lacking the decryption key

Honeynet - a fake network that distracts hackers to prevent them from accessing the real network

Security policy - a company policy that defines what users can and cannot do on the company network and how the company should manage security